

58, 973  
10/518973

特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004年11月4日 (04.11.2004)

PCT

(10) 国際公開番号  
WO 2004/095772 A1

(51) 国際特許分類: H04L 9/32, G06F 15/00

(21) 国際出願番号: PCT/JP2004/005741

(22) 国際出願日: 2004年4月21日 (21.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2003-115755 2003年4月21日 (21.04.2003) JP  
特願2003-188141 2003年6月30日 (30.06.2003) JP

(71) 出願人(米国を除く全ての指定国について): ソニー  
株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001  
東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および  
(75) 発明者/出願人(米国についてのみ): 三浦 貴之  
(MIURA, Takayuki) [JP/JP]. 小野剛 (ONO, Tsuyoshi) [JP/JP]. 鈴木直志 (SUZUKI, Naoshi) [JP/JP]. 宮田耕  
自 (MIYATA, Kouji) [JP/JP].

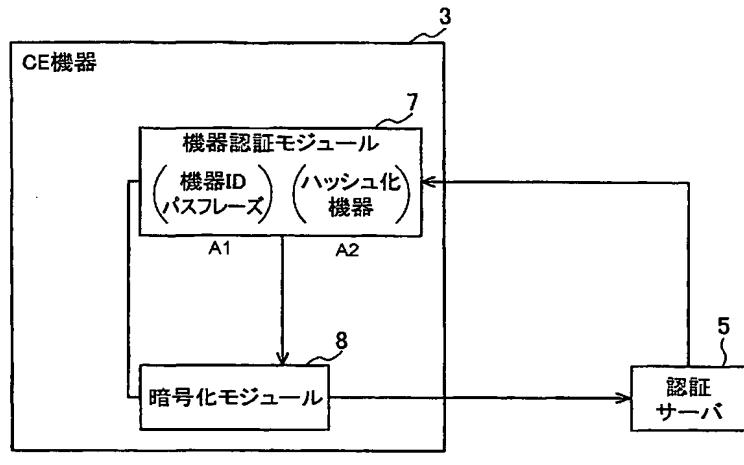
(74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒  
1050001 東京都港区虎ノ門1丁目2番3号虎ノ門第一  
ビル9階三好内外国特許事務所内 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が  
可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,  
BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,  
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,  
ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,

(統葉有)

(54) Title: DEVICE AUTHENTICATION SYSTEM

(54) 発明の名称: 機器認証システム



(57) Abstract: In a CE device, it is possible to connect a device authentication module with an encryption module by a dynamic link. An authentication server (5) generates a random number. A device authentication module (7) creates a digest by combining a path phrase with this random number and transmits the digest and the device ID to an encryption module (8). The encryption module encrypts the communication path and transmits these information to an authentication server (5). The authentication server (5) searches the path phrase from the device ID and combines this with the random number previously generated, thereby creating a digest. This digest is compared to the digest received from the encryption module (8), thereby performing device authentication. The encryption module (8) can be connected by a dynamic link instead of a static link so as to receive a digest instead of a path phrase from the device authentication module (7).

(57) 要約: CE機器において、機器認証モジュールと暗号化モジュールをダイナミックリンクにて接続できること。認証サーバ(5)で乱数を発生させる。機器認証モジュール(7)はパスフレーズとこの乱数を組み合わせてダイジ

(統葉有)

WO 2004/095772 A1



LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 國際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,

---

ストを生成し、これと機器IDを暗号化モジュール(8)に渡す。暗号化モジュールは、通信経路を暗号化し、これら情報を認証サーバ(5)に送信する。認証サーバ(5)は、機器IDからパスフレーズを検索し、これと先に生成した乱数を組み合わせてダイジェストを生成する。このダイジェストと暗号化モジュール(8)から受信したダイジェストを比較して機器認証を行う。暗号化モジュール(8)は、機器認証モジュール(7)からパスフレーズではなくダイジェストを受け取るため、スタティックリンクにて接続せずにダイナミックリンクで接続することができる。

## 明細書

機器認証システム

機器認証システム、端末機器、認証サーバ、サービスサーバ、端末機  
5 器方法、認証方法、端末機器プログラム、認証プログラム、サービスサ  
ーバプログラム、及び記憶媒体

## 技術分野

本発明は、認証システムなどに関し、特に、セキュリティ上重要な情  
10 報を所定のロジックで変換し、変換後の情報を用いて認証するものに関する。

## 背景技術

近年、CE (C E : C o n s u m e r E l e c t r o n i c s) 機  
15 器の普及が広まりつつある。CE機器とは、例えば、ビデオデッキ、ハ  
ードディスクレコーダ、ステレオ、テレビなどのオーディオビジュアル  
機器や、パーソナルコンピュータ、デジカメ、カムコーダ、P D A 、ゲ  
ーム機、ホームルータ等の電子機器や、炊飯器、冷蔵庫などの家電製品  
や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介  
20 したサービスを利用するものである。

そして、CE機器からサーバにアクセスしてコンテンツをダウンロー  
ドしたり、サービスを受けるなどし、ユーザはサーバが提供するサービ  
スを利用することができる。

サーバが提供するサービスには、CE機器全般に提供するものと、機  
25 器認証された特定のCE機器に提供するものがある。

サーバは、機器認証を要するサービスを提供する場合、そのCE機器

を認証サーバで認証し、認証された場合にサービスを提供する。

このように、サービスサーバが端末機器にサービスを提供するものとして次の発明がある。

特許文献 1：特開 2002-342285 号公報

5 この発明は、端末機器（携帯電話）から認証要求があった場合に、これを認証すると共に端末機器にワンタイムパスワードを発行して送信する。端末機器から情報の要求があった場合、端末機器から先のワンタイムパスワードを受信し、認証したのが確かにこの端末機器であるかを確認するものである。

10 図 12 は、従来の CE 機器 101 の構成を示した図である。CE 機器 101 は、機器 ID やパスフレーズなどの認証に必要な認証情報を記憶していると共に、機器認証に関する処理を行う機器認証モジュール 103 と、機器認証モジュール 103 から認証情報を受け取り、通信経路を暗号化してこれを機器認証先 105 に送信する暗号化モジュール 104 15 を備えている。

機器認証モジュール 103 は、暗号化モジュール 104 に認証情報を平文で渡すため、この認証情報が第三者に読み取られないように、機器認証モジュール 103 と暗号化モジュール 104 はスタティックリンクにて結合されている。

20 通信経路を暗号化するモジュールは、機器認証以外の用途で利用する場合も多いが、暗号化モジュール 104 は機器認証モジュール 103 とスタティックリンクされているため、CE 機器 101 は、これとは別に機器認証以外の用途で使用する暗号化モジュールを用意している。

25 このように、CE 機器 101 では、同じ機能を有する 2 つの暗号化モジュールを CE 機器 101 内のメモリに実装しなくてはならず、実質として機器認証モジュールの容量が多くなり、CE 機器 101 の利用可能な

メモリ領域を圧迫したり、あるいは機器認証機能の実装そのものが困難となる場合があった。

そこで、本発明の目的は、端末機器内のメモリを有効利用することができる機器認証機能を実現できる端末機器認証システムなどを提供する  
5 ことである。

### 発明の開示

機器認証用の秘密情報を備えた端末機器と、前記秘密情報を用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方向性関数により変換して変換値を生成し、前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、前記取得した乱数と秘密情報との組を前記端末機器が用いた一方向性関数と同じ一方向性関数により変換して変換値を生成し、前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システムを提供する（第1の構成）。

また、本発明は、第1の構成の機器認証システムで機器認証を受ける端末機器が、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報を、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するよう構成することもできる（第2の構成）。

また、本発明は、第2の構成の端末機器を機器認証する認証サーバが、

乱数を取得する乱数取得手段と、前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信手段と、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信手段と、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第3の構成）。

また、本発明は、第1の構成の機器認証システムが、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、前記サービスサーバが、乱数を取得する乱数取得手段と、前記取得した乱数を端末機器に送信する乱数送信手段と、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、を具備するように構成することもできる（第4の構成）。

また、本発明は、第4の構成のサービスサーバからサービスの提供を受ける端末機器が、サービスサーバから乱数を受信する乱数受信手段と、前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するように構成することもできる（第5の構成）。

また、本発明は、第4の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第6の構成）。

また、本発明は、第1の構成の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

また、本発明は、第2の構成の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記受信

した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。

また、本発明は、第4の構成のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信ステップと、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、から構成された認証方法を提供する。

また、本発明は、第4の構成のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、前記受信した乱数と、秘密情報の組を前記変換手段で

一方向性関数により変換して変換値を生成する変換ステップと、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

5 また、本発明は、第4の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが用いる認証方法であって、前記認証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を前記受信手段で受信する受信ステップと、前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定ステップと、前記受信した乱数と前記特定した秘密情報との組を前記変換手段で前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記機器認証手段で、  
10 前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。  
15

また、本発明は、第1の構成の機器認証システムで機器認証を受けるコンピュータで構成された端末機器において、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信機能と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、を実現する端末機器プログラムを提供する。

また、本発明は、第2の構成の端末機器を機器認証するコンピュータで構成された認証サーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信

する送信機能と、前記端末機器から、変換値と、前記乱数特定情報と、  
秘密情報特定情報を受信する受信機能と、前記受信した乱数特定情報を  
用いて前記端末機器に送信した乱数を特定する乱数特定機能と、前記受  
信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘  
5 密情報特定機能と、前記特定した秘密情報と乱数の組を、前記端末機器  
が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成  
する変換機能と、前記受信した変換値と前記生成した変換値を用いて前  
記端末機器を機器認証する機器認証機能と、を実現する認証プログラム  
を提供する。

10 また、本発明は、第4の構成のコンピュータで構成されたサービスサ  
ーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数を端  
末機器に送信する乱数送信機能と、前記端末機器から、秘密情報を用い  
て生成した変換値と、秘密情報特定情報を受信する受信機能と、前記端  
末機器に送信した乱数を特定する乱数特定機能と、前記受信した変換値  
15 と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サ  
ーバに送信する認証情報送信機能と、前記認証サーバから前記送信した  
認証情報による認証結果を受信する認証結果受信機能と、を実現するサ  
ービスサーバプログラムを提供する。

また、本発明は、第4の構成のサービスサーバからサービスの提供を  
20 受けるコンピュータで構成された端末機器において、サービスサーバか  
ら乱数を受信する乱数受信機能と、前記受信した乱数と、秘密情報の組  
を一方向性関数により変換して変換値を生成する変換機能と、前記生成  
した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密  
情報特定情報を送信する送信機能と、を実現する端末機器プログラムを  
25 提供する。

また、本発明は、第4の構成のサービスサーバがサービスを提供する

際に、端末機器を機器認証するコンピュータで構成された認証サーバにおいて、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、を実現する認証プログラムを提供する。

また、本発明は、上記各プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本発明は、請求項1の機器認証システムで機器認証を受ける端末機器であって、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備し、前記秘密情報と、前記変換手段は、端末機器に組み込まれた耐タンパ装置に格納されていることを特徴とする端末機器を提供する。

## 20 図面の簡単な説明

図1は、本実施の形態の機器認証システムの構成を説明するための図である。

図2は、CE機器の機器認証に関する構成要素を説明するための図である。

25 図3は、CE機器のハードウェア的な構成の一例を示した図である。

図4は、機器認証を行う手順を説明するためのフローチャートであ

る。

図 5 は、ダイジェスト認証処理の手順を説明するためのフローチャートである。

図 6 は、サービスサーバが認証サーバで認証結果を確認する手順を 5 説明するためのフローチャートである。

図 7 は、CE 機器が認証サーバを確認する別のシーケンスを説明するためのフローチャートである。

図 8 は、機器認証を行う他の手順を説明するためのフローチャートである。

10 図 9 は、ダイジェスト認証処理の手順を説明するためのフローチャートである。

図 10 は、本実施の形態の変形例を説明するための図である。

図 11 は、本変形例のハードウェア的な構成の一例を示した図である。

15 図 12 は、従来の CE 機器の構成を説明するための図である。

### 発明を実施するための最良の形態

以下、本発明の好適な実施の形態について、図を参照して詳細に説明 20 する。

#### (1) 実施形態の概要

図 2 に示したように、機器認証モジュール 7 は、認証サーバ 5 からサーバ乱数とワンタイム ID を受信し、このサーバ乱数とパスフレーズを組み合わせてハッシュ化してダイジェストを生成する。そして、これを 25 機器 ID と共に暗号化モジュール 8 に渡す。暗号化モジュール 8 は、通信経路を暗号化し、ダイジェストと機器 ID、及びワンタイム ID を認

証サーバ5に送信する。

認証サーバ5は、予め機器IDとCE機器3のパスフレーズを対応付けて記憶している。また、先にCE機器3に送信したサーバ乱数とワンタイムIDを対応付けて記憶している。

5 認証サーバ5は、CE機器3から受信したワンタイムIDと機器IDを用いてパスフレーズと先に発生したサーバ乱数を特定する。そしてこれらを組み合わせ、CE機器3側のロジックと同じロジックでダイジェストを生成する。そして、生成したダイジェストとCE機器3から受信したダイジェストを照合し、両者が一致するか否かでCE機器3の認証

10 行う。

このように、機器認証モジュール7は、暗号化モジュール8にパスフレーズを渡さずに、サーバ乱数とパスフレーズの組から生成したダイジェストを渡す。そのため、機器認証モジュール7から第三者によりダイジェストが読み取られたとしても第三者はダイジェストからパスフレー

15 ズを復元することはできない。

更に、認証サーバ5は、機器認証の度に異なるサーバ乱数を生成するため、機器認証モジュール7が暗号化モジュール8に渡すダイジェストも機器認証ごとに異なり、例えダイジェストが第三者に読み取られたとしてもこれを乱用されることはない。

20 また、機器認証の度に同じダイジェストを用いる第三者にこのダイジェストが漏れた場合、これを元に所謂リプレイ攻撃が行われる可能性があるが、CE機器3は、機器認証の度に異なるダイジェストを生成するのでリプレイ攻撃されることはない。

## (2) 実施形態の詳細

25 図1は、本実施の形態の機器認証システム1の構成を説明するための図である。

機器認証システム1は、CE機器3、サービスサーバ4、認証サーバ5がネットワークを介して通信可能に接続されている。

なお、図1ではCE機器3とサービスサーバ4が一台ずつ記載されているが、これは複数存在させることができる。

5 CE機器3は、機器ID、パスフレーズなど機器認証に必要な認証情報を持てており（記憶装置3aに記憶してある、図3の記憶部28に対応）、これらの情報を用いて認証サーバ5で機器認証を受け、サービスサーバ4が提供するサービスを利用することができる。

なお、パスフレーズは、CE機器3と認証サーバ5が機器認証のため10に共有する秘密情報を構成している。

サービスサーバ4は、CE機器3に、例えば、コンテンツを送信するなどサービスを提供するサーバである。サービスサーバ4が提供するサービスには機器認証を要するものと要しないものがある。CE機器3が機器認証を要するサービスを要求した場合、サービスサーバ4は、認証15サーバ5に機器認証を代行してもらう。

サービスサーバ4は、サービスを提供するCE機器3を登録しており、サービスサーバ4に接続可能な各CE機器の機器情報（シリアルナンバーなど）、保有者情報などを記憶装置4aに記憶している。これらの情報は、CE機器3から認証結果を受信した際に、認証サーバ5に機器認証20を受けたCE機器3が本当にこのCE機器3であるか確認するのに用いる。

認証サーバ5は、サービスサーバ4に代わってCE機器3の機器認証を代行するサーバである。

認証サーバ5は、乱数（以下、サーバ乱数と呼ぶことにする）を生成25してCE機器3に送信し、CE機器3から機器ID、及びサーバ乱数とパスフレーズから生成したダイジェストなどを受信し、CE機器3の機

器認証を行う。認証サーバ5は、認証ごとに毎回異なったサーバ乱数を生成する。

認証サーバ5は、乱数を発生させることによりこれを取得する乱数取得手段を備えているが、認証サーバ5は、他の装置が生成した乱数取得するように構成することもできる。

認証サーバ5は、各CE機器3ごとにパスフレーズ、機器ID、機器情報、保有者情報などを記憶装置5aに記憶しているほか、サービスサーバ4がCE機器3にサービスを提供するサービスサイトのURL (Uniform Resource Locators)も記憶している。

このURLは、CE機器3が利用しようとしているサイトが適切なものか否かを判断するために、予めサービスサーバ4が取得して登録したものである。

認証サーバ5は、CE機器3から機器IDを受信、この機器IDにひも付けられたパスフレーズを検索することにより、CE機器3のパスフレーズを取得する。このように、機器IDはCE機器3の秘密情報（パスフレーズ）を特定する秘密情報特定情報を構成している。

サービスサーバ4のほかに機器認証を行う認証サーバ5を設けたのは（従来はサービスサーバ4が機器認証も行っていた）、サービスサーバ4は一般の個人や任意の団体などが運営する場合も多く、認証情報をサービスサーバ4に提供した場合、提供した情報が悪用されてしまう可能性があるためである。

このように、機器認証の代行を行う認証サーバ5を設けたシステムとしては未公開の文献（特願2002-144896）で提案されているサービス提供システムがある。

このシステムでは、機器認証を機器認証サーバが一括して行い、サービスサーバは、機器認証サーバでの認証結果を受け取って、CE機器に

サービスを提供するか否かを判断する。

このシステムでは、機器認証を行う場合にセキュリティ上重要な情報を機器認証サーバに送信するため、これらの情報をサービスサーバに提供する必要がない。

5 図2は、CE機器3を構成する要素のうち、機器認証に関するものを説明するための図である。

CE機器3は、機器認証モジュール7と暗号化モジュール8を備えている。機器認証モジュール7は、機器IDやパスフレーズなど、機器認証に必要な認証情報を記憶している。また、機器認証モジュール7は、  
10 認証サーバ5からサーバ乱数の受信し、これとパスフレーズを組み合わせてハッシュ化し、ダイジェスト（ハッシュ値、あるいはダイジェストメッセージ）を生成することができる。

機器認証モジュール7は、認証情報として機器IDとダイジェストを暗号化モジュール8に渡す。

15 ここでハッシュ化とは、ハッシュ関数と呼ばれる関数を用いて電子文書から文字列（ダイジェスト）を生成する処理のことである。

同じ電子文書からは同じダイジェストが得られる。電子文書が一部でも変更されると、この文書のダイジェストは、変更前のものと異なる。また、ダイジェストから元の電子文書を復元することはできない。

20 なお、ハッシュ関数は一方向性関数と呼ばれる関数の一種である。一方向性関数とは、変換元から変換値への変換は容易であるが、変換値から変換元への逆変換が困難な関数である。そして、ダイジェストは、変換元（パスフレーズとサーバ乱数の組）をハッシュ関数で変換した変換値となる。

25 このように、CE機器3は、乱数（サーバ乱数）と秘密情報（パスフレーズ）の組を一方向性関数で変換し変換値（ダイジェスト）を取得す

る変換手段を備えている。

暗号化モジュール8は、例えば、SSL (S e c u r e S o c k e t s L a y e r)などの暗号化技術を使って、通信経路を暗号化するモジュールである。暗号化モジュール8は、機器認証モジュール7から  
5 認証情報を受け取り、暗号化した通信経路を経由して認証サーバ5に認証情報を送信する。

このように、CE機器3では、機器認証モジュール7から出力されるパスフレーズは、サーバ乱数と組にして生成されたダイジェストとなっている。そのため、機器認証モジュール7から暗号化モジュール8に渡  
10 される認証情報には、平文のパスフレーズが含まれておらず、認証情報が第三者に渡ったとしても、ダイジェストからパスフレーズを復元することはできない。更に、機器認証に使用するダイジェストは毎回変化するので、第三者がダイジェストを読み取ってもこれを乱用することはできない。そのため高いセキュリティを確保することができる。

15 機器認証モジュール7と暗号化モジュール8は、ダイナミックリンクにより接続される。

即ち、暗号化モジュール8は、機器認証モジュール7が認証情報を認証サーバ5に送信する際に暗号化モジュール8に動的に接続される。

そのため、暗号化モジュール8は、機器認証モジュール7とは別の通信経路を暗号化する必要があるモジュールからも利用できる。

その場合は、そのモジュールが暗号化した通信経路で情報を送信する場合に暗号化モジュール8が動的にそのモジュールに接続する。

このように、暗号化モジュール8は、複数のモジュールから共用することができ、CE機器3のメモリ領域を節約することができる。

25 図3は、CE機器3のハードウェア的な構成の一例を示した図である。

CPU(Central Processing Unit)21は、

ROM (Read Only Memory) 22に記憶されているプログラム、または記憶部28からRAM (Random Access Memory) 23にロードされたプログラムに従って各種の処理を実行する。

5 また、RAM 23には、CPU 21が各種の処理を実行する上で必要なデータなども適宜記憶されている。

CPU 21、ROM 22、およびRAM 23は、バス24を介して相互に接続されている。このバス24には、入出力インターフェース25も接続されている。

10 入出力インターフェース25には、キーボード、マウスなどよりなる入力部26、CRT (Cathode-ray Tube)、LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどによりなる出力部27、ハードディスクなどにより構成される記憶部28、モデム、ターミナルアダプタなどにより構成される通信部29が接続されている。通信部29は、ネットワークを介しての通信処理を行う。

20 また、入出力インターフェース25には、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、またはメモリカード44などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

なお、認証サーバ5、サービスサーバ4の構成は基本的にCE機器3と同様であるので説明は省略する。

25 図4は、CE機器3が認証サーバ5から機器認証を受ける手順を説明するためのフローチャートである。

なお、CE機器3は、認証サーバ5の公開鍵を備えており、認証サー

バ5は対応する秘密鍵を備えているものとする。

また、CE機器3と認証サーバ5は、フローチャート中の括弧で示した各手段を備えている。

CE機器3がサービスサーバ4で機器認証が必要なサービスにアクセスすると、サービスサーバ4がCE機器3に機器認証トリガを送信する(ステップ40)。

この機器認証トリガは、CE機器3に機器認証動作を開始させるための情報であり、認証サーバ5のURLや、サービスサイトが要求する認証のバージョンなどの情報が含まれている。

なお、機器認証にはいくつかのバージョンが用意されており、バージョンにより利用できるサービスが異なる場合がある。

CE機器3は、サービスサーバ4から認証トリガを受信する。

以下の、CE機器3と認証サーバ5の通信は、暗号化モジュール8で暗号化された通信経路を介して行われる。

CE機器3は、認証トリガに含まれる認証サーバ5のURLを用いて認証サーバ5に接続し、サーバ乱数の送信を要求する(ステップ2)。

また、このとき、CE機器3は、認証トリガに含まれているサービスサーバ4が要求するバージョンと、CE機器3が実装している機器認証のバージョンを認証サーバ5に送信する。

認証サーバ5は、CE機器3からサーバ乱数の送信要求を受信し、サーバ乱数を発生させる(乱数取得手段)(ステップ20)。また、サービスサーバ4が要求しているバージョンとCE機器3のバージョンが一致しているか否かの確認も行う。

更に、認証サーバ5は、ワンタイムID1を生成する。そして、サーバ乱数とワンタイムID1をCE機器3に送信する(送信手段)(ステップ22)。

なお、サービスサーバ4は後ほど別のワンタイムIDを生成するが、これと区別するため、上記のワンタイムIDをワンタイムID1とし、後に生成するワンタイムIDをワンタイムID2とする。

このワンタイムID1は、CE機器3と認証サーバ5でセッションを5維持するために使用される使い捨てのIDである。

認証サーバ5は、CE機器3からワンタイムID1を受信することによりCE機器3と維持しているセッションを認識することができる。

ワンタイムID1は、機器認証ごとに異なる値が発行されるので、高いセキュリティを確保することができる。

10 また、認証サーバ5は、送信したサーバ乱数とワンタイムID1をひも付けして記憶する。これにより、後にCE機器3からワンタイムID1を受信することにより、CE機器3に送信したサーバ乱数を特定することができる。このように、ワンタイムID1は、乱数特定情報を構成している。

15 CE機器3は、認証サーバ5からサーバ乱数とワンタイムID1を受信する（受信手段）。ついで、CE機器3は、共通鍵を生成してこれを認証サーバ5の公開鍵で暗号化する（ステップ4）。この情報は、CE機器3の接続先が確かに認証サーバ5であることを確認するために用いられる。

20 次に、CE機器3は、パスフレーズとサーバ乱数を組み合わせて所定のロジックでハッシュを取り、ダイジェストを生成する（変換手段）（ステップ6）。

次に、CE機器3は、機器ID、生成したダイジェスト、認証サーバ5から受信したワンタイムID1を認証サーバ5を送信する（送信手段）25（ステップ8）。

また、これらの情報と共に、先に公開鍵で暗号化した共通鍵と、CE

機器 3 がサービスを受けようとしているサービスサーバ 4 のサイトの U R L (以下ターゲット U R L と呼ぶ) 、及び、共通鍵を取り出すための秘密鍵 (認証サーバ 5 は、複数の秘密鍵を持っている) を識別する秘密鍵識別子も認証サーバ 5 に送信する。

5 認証サーバ 5 は、これら情報を C E 機器 3 から受信して(受信手段)、まずワンタイム I D 1 の確認を行う (ステップ 24) 。ワンタイム I D 1 により、認証サーバ 5 は、先に生成したセッションの続きであることを認識することができる。

また、ワンタイム I D 1 にひも付けて置いたサーバ乱数を記憶装置から10 取得することによりサーバ乱数を特定する (乱数特定手段) 。

また、機器 I D から C E 機器 3 のパスフレーズを特定する (秘密情報特定手段) 。

更に、認証サーバ 5 は、C E 機器 3 から受信したターゲット U R L が、予め認証サーバ 5 に登録されているターゲット U R L かも確認する。

15 これにより、C E 機器 3 の接続先のサービスサーバ 4 が正当なサービスサーバ 4 であることを確認することができる。

次に、認証サーバ 5 は、先に C E 機器 3 に送信したサーバ乱数と、C E 機器 3 のパスフレーズから、C E 機器 3 と同じロジックによりダイジ20 ェストを生成し (変換手段) 、これと、C E 機器 3 から受信したダイジエストを照合して C E 機器 3 の認証を行う (機器認証手段) (ステップ 26) 。

認証サーバ 5 は、認証に成功するとワンタイム I D 2 を生成する (ステップ 28) 。ワンタイム I D 2 は、後ほど C E 機器 3 が認証を受けたのが確かに認証サーバ 5 であることをサービスサーバ 4 が確認するのに25 使用される。

また、認証サーバ 5 は、機器認証を行ったバージョンも記憶しておく。

次に、認証サーバ5は、公開鍵で暗号化された共通鍵を秘密鍵で復号化して取り出す。

そして、認証サーバ5は、ワンタイムID2をハッシュ化し、ダイジェスト（以下、ID2ダイジェストと呼ぶ）を生成する。

5 次に、認証サーバ5は、ID2ダイジェストを先に復号化した共通鍵で暗号する（ステップ30）。

次に、認証サーバ5は、暗号化したID2ダイジェストと、ワンタイムID2を連結して共通鍵で暗号化し、これをCE機器3に送信する（ステップ32）。

10 ワンタイムID2にID2ダイジェストを連結するのは、送信されてきたワンタイムID2のダイジェストを生成して、ID2ダイジェストと比較することにより、ワンタイムID2が改変されたか否かを確認するためである。

CE機器3は、認証サーバ5から暗号化されたワンタイムID2とID2ダイジェストを受信し、共通鍵でこれらを復号化する（ステップ10）。

CE機器3は、ワンタイムID2をハッシュ化してダイジェストを生成し、これをID2ダイジェストと比較してワンタイムID2が改竄されていないか確認する。

20 CE機器3は、共通鍵でこれらの情報が復号化できたことから、認証サーバ5が共通鍵を取り出せた（即ち、秘密鍵を持っている）ことを確認することができる。即ち、CE機器3が機器認証を求めた相手先は確かに認証サーバ5であった

ことを確認することができる（ステップ12）。

25 また、ワンタイムID2が発行されたことから、CE機器3が機器認証されたことを確認することができる。

次に、CE機器3は、認証サーバ5から受信したワンタイムID2をサービスサーバ4に送信することにより、CE機器3が認証サーバ5で認証されたことを通知する（ステップ14）。

サービスサーバ4は、CE機器3からワンタイムID2を受信し、これ5を認証サーバ5に送信して確かに認証サーバ5が機器認証したこと5を確認する（ステップ34、ステップ42）。

サービスサーバ4は、認証サーバ5で機器認証結果を確認すると、CE機器3に対してサービスの提供を開始する（ステップ44）。

そして、CE機器3ではサービスの利用を開始する（ステップ16）。

以上の手順により、認証サーバ5は、パスフレーズそのものではなく、10パスフレーズとサーバ乱数から生成されるダイジェストによりダイジェスト認証を行うことができる。

また、CE機器3は、共通鍵を公開鍵で暗号化して認証サーバ5に送信し、認証サーバ5の秘密鍵で共通鍵が取り出されたことを確認することにより、認証先が確かに認証サーバ5であることを確認することができる。

更に、認証サーバ5は、ワンタイムID2にID2ダイジェストを貼付してCE機器3に送信することにより、CE機器3は、ワンタイムID2が改竄されていないことを確認することができる。

20 図5は、ステップ26（図4）のダイジェスト認証処理の手順を説明するためのフローチャートである。

認証サーバ5は、CE機器3へサーバ乱数とワンタイムID1を送信する際に、これらを対応付けて記憶している。

認証サーバ5は、CE機器3から受信したワンタイムID1を用いて25CE機器3に送信したサーバ乱数を検索する（ステップ52）。

また、認証サーバ5は、機器IDとパスフレーズを予め対応付けて記

憶しており、C E 機器 3 から受信した機器 I D から C E 機器 3 のパスフレーズを検索する（ステップ 5 4）。

次に、認証サーバ 5 は、検索したサーバ乱数とパスフレーズの組を C E 機器 3 と同じロジックによりハッシュ化し、ダイジェストを生成する 5（ステップ 5 6）。

次に、認証サーバ 5 は、生成したダイジェストと、C E 機器 3 から受信したダイジェストを比較し、同一か否かを判断する（ステップ 5 8）。

ダイジェストが一致した場合（ステップ 6 0；Y）、認証サーバ 5 は、機器認証が成功したことを認識する（ステップ 6 2）。

10 ダイジェストが一致しなかった場合（ステップ 6 0；N）、認証サーバ 5 は、C E 機器 3 が認証されなかったものと認識する（ステップ 6 4）。

以上のように、認証サーバ 5 は、ワンタイム I D とサーバ乱数を対応付けて記憶しておく、更に機器 I D とパスフレーズを対応付けて記憶しておくことにより、C E 機器 3 と同じロジックでダイジェストを生成す 15 ることができ、C E 機器 3 を機器認証することができる。

図 6 は、ステップ 3 4、ステップ 4 2（図 4）において、サービスサーバ 4 が認証サーバ 5 で認証結果を確認する手順を説明するためのフローチャートである。

以下、認証サーバ 5 とサービスサーバ 4 の通信は、S S L などの技術 20 により暗号化された通信経路を介して行われるものとする。

まず、サービスサーバ 4 は、認証サーバ 5 に C E 機器 3 から受信したワンタイム I D 2 を送信し、機器認証の結果を要求する（ステップ 8 2）。この際に、サービスサーバ 4 は、認証サーバ 5 とのセッションを維持するためのチケットを発行し、これも認証サーバ 5 に送信する。

25 サービスサーバ 4 と認証サーバ 5 との送受信はお互いの信頼性が高いため、セッションの度にワンタイム I D を発行せず、同じ I D を複数回

繰り返して使用してもよい。このように複数回再利用できる I D をチケットと呼ぶことにする。

ワンタイム I D の代わりにチケットを発行することにより、サービスサーバ 4 と認証サーバ 5 の負荷を、ワンタイム I D を発行した場合より 5 小さくすることができる。

認証サーバ 5 は、ワンタイム I D 2 を受信し、このワンタイム I D 2 をキーとして、C E 機器 3 に対して行った機器認証のバージョンを検索する。また、C E 機器 3 の機器 I D などから C E 機器 3 の機器情報も検索する。

10 機器情報としては、例えば、C E 機器 3 の製品コードやシリアルナンバなどがある。

そして、これら検索した情報をサービスサーバ 4 に送信する（ステップ 7 2）。

サービスサーバ 4 は、バージョン情報と機器情報を認証サーバ 5 から 15 受信し、サービスサーバ 4 で記憶しているこれらの情報と照合する。

更に、サービスサーバ 4 は、認証サーバ 5 にチケットを送信し、C E 機器 3 の保有者情報を認証サーバ 5 に要求する（ステップ 8 4）。

認証サーバ 5 は、これに応じてこのC E 機器 3 の保有者情報を検索し、チケットと共にサービスサーバ 4 に送信する（ステップ 7 4）。

20 サービスサーバ 4 は、認証サーバ 5 から受信した保有者情報をサービスサーバ 4 が記憶している保有者情報と照合する。

このように、機器情報や保有者情報を確認することにより、サービスサーバ 4 は、認証サーバ 5 は、確かに C E 機器 3 を機器認証したこと 25 を確認することができる。

そして、サービスサーバ 4 は、C E 機器 3 に対してサービスの提供を開始する（ステップ 8 6）。

以上のように、サービスサーバ4と認証サーバ5との間の複数回の送受信において同じチケットが繰り返し用いられる。

また、サービスサーバ4は、別の機器認証に関する認証結果確認には別のチケットを発行する。

5 図7は、CE機器3が認証先が確かに認証サーバ5であることを確認する別のシーケンスを説明するためのフローチャートである。

以下の手順では、CE機器3が乱数（以下クライアント乱数と呼ぶこととする）を発生させ、これにより認証サーバ5を確認する。

まず、CE機器3は、クライアント乱数を生成する（ステップ102）。

10 次に、CE機器3は、共通鍵を生成する（ステップ104）。

CE機器3は、生成した共通鍵でクライアント乱数を暗号化する（ステップ106）。暗号化した後の情報を暗号化情報1と呼ぶこととする。

更に、CE機器3は、認証サーバ5の公開鍵で共通鍵を暗号化する（ステップ108）。暗号化した後の情報を暗号化情報2と呼ぶこととする。

15 そして、CE機器3は、暗号化情報1と暗号化情報2を認証サーバ5に送信する（ステップ110）。

なお、CE機器3は、送信したクライアントを記憶しておく。

認証サーバ5は、CE機器3から暗号化情報1と暗号化情報2を受信し、まず、認証サーバ5の秘密鍵で暗号化情報2を復号化し、共通鍵を取り出す（ステップ122）。

次に、認証サーバ5は、取り出した共通鍵で暗号化情報1を復号化し、クライアント乱数を取り出す（ステップ124）。

次に、認証サーバ5は、取り出したクライアント乱数のハッシュをとり、ダイジェストを生成する（ステップ126）。

25 次に、認証サーバ5は、生成したダイジェストを共通鍵で暗号化し、CE機器3に送信する（ステップ128）。

CE 機器 3 は、認証サーバ 5 から暗号化したダイジェストを受信し、これを共通鍵で復号化する（ステップ 112）。

更に、CE 機器 3 は、記憶しておいた乱数をハッシュ化し、ダイジェストを生成する（ステップ 114）。

5 そして、CE 機器 3 は、生成したダイジェストと、先に復号化したダイジェストを比較し、両者が一致することにより、接続先が確かに認証サーバ 5 であることを確認する（ステップ 116）。

即ち、クライアント乱数のダイジェストが共通鍵で暗号化されて送られてきたということは、接続先が暗号化情報 2 を復号化することができ  
10 たということであり、これは、接続先が秘密鍵を持っていたことを意味する。秘密鍵を持っているのは認証サーバ 5 であるので、これにより、接続先が認証サーバ 5 であることを確認することができる。

図 8 は、機器認証を行う他の手順を説明するためのフローチャートである。

15 図 4 に示した手順では、CE 機器 3 から認証サーバ 5 にアクセスして機器認証を行ったが、この手順では、CE 機器からサービスサーバ 4 に認証情報を送信し、サービスサーバ 4 がこの認証情報を用いて認証サーバ 5 にアクセスして機器認証を行う。

20 以下の手順で、CE 機器 3、サービスサーバ 4、認証サーバ 5 の間の通信は、例えば、SSL などの技術により暗号化した経路が用いられるものとする。

また、CE 機器 3、サービスサーバ 4、認証サーバ 5 は、フローチャート中に括弧で示した各手段を備えている。

25 まず、CE 機器 3 がサービスサーバ 4 に対して機器認証を要するサービスの提供を要求する。

これに対し、サービスサーバ 4 は、CE 機器 3 に対して機器認証トリ

ガを送信する（ステップ142）。

CE機器3は、サービスサーバ4から機器認証トリガを受信するとサービスサーバ4に対してサーバ乱数の要求を送信する（ステップ132）。

サービスサーバ4は、これを受信してサーバ乱数を生成し（乱数取得手段）（ステップ144）、CE機器3に送信する（乱数送信手段）（ステップ146）。サービスサーバ4は、このサーバ乱数を記憶しておく。

CE機器3は、サービスサーバ4からサーバ乱数を受信すると共に（乱数受信手段）、クライアント乱数を生成する（ステップ134）。

次にCE機器3は、サーバ乱数、クライアント乱数、及びパスフレーズを組み合わせてハッシュ化し、ダイジェストを生成する（変換手段）（ステップ136）。

次に、CE機器3は、生成したダイジェストと、機器ID、クライアント乱数をサービスサーバ4に送信して機器認証を要求する（送信手段）（ステップ138）。

サービスサーバ4は、これらの認証情報を受信する（受信手段）（ステップ148）。

このように、サービスサーバ4がCE機器3から受信する認証情報には、サーバ乱数が含まれていない。

サービスサーバ4は、CE機器3から受信した認証情報（ダイジェスト、機器ID、クライアント）にサーバ乱数を加えて新たな認証情報とし、これを認証サーバ5に送信して機器認証を要求する（認証情報送信手段）（ステップ150）。

ここでは、サービスサーバ4は、CE機器3とセッションを維持しているため、先に記憶したサーバ乱数がこのCE機器3に送ったサーバ乱数であることを認識することができる（乱数特定手段）。そこで、このサーバ乱数を認証情報に加えるのである。また、図4の手順と同様にし

てワンタイム ID を発行することにより、CE 機器 3 に送信したサーバ乱数を特定するように構成することもできる。

このように、CE 機器 3 から送られてきた認証情報に先に送信したサーバ乱数を付加するように構成することにより、認証トリガを送信した 5 サービスサーバ 4 と認証情報を受信したサービスサーバ 4 が同一のサーバであることを確かめることができる。

認証サーバ 5 は、サービスサーバ 4 から認証情報を受信し(受信手段)、CE 機器 3 の機器認証を行う(ステップ 162)。

この認証では、サービスサーバ 4 から送信されてきた機器 ID、クラ 10 イアント乱数、サーバ乱数の組から、CE 機器 3 と同じロジックでダイジェストを生成し、サービスサーバ 4 から送信されてきたダイジェストと一致するか否かをチェックする。

一致した場合、CE 機器 3 は認証され、一致しない場合は認証されない。

15 そして、認証サーバ 5 は、認証結果をサービスサーバ 4 に送信する(ステップ 164)。

また、CE 機器 3 のパスフレーズは、機器 ID から求める(秘密情報特定手段)。

サービスサーバ 4 は、認証サーバ 5 から認証結果を受信し(認証結果受信手段)、その認証結果が CE 機器 3 を認証するものであった場合、サービスの提供を開始し(ステップ 152)、CE 機器 3 ではそのサービスを利用する(ステップ 140)。

なお、ステップ 164 で認証サーバ 5 がサービスサーバ 4 に認証結果を送信する際に、図 6 のフローチャートと同様にして、認証サーバ 5 と 25 サービスサーバ 4 の間で CE 機器 3 の機器情報と保有者情報を確認するように構成することもできる。

図9は、ステップ162(図8)のダイジェスト認証処理の手順を説明するためのフローチャートである。

まず、認証サーバ5は、サービスサーバ4から受信した認証情報に含まれる機器IDを用いてCE機器3のパスフレーズを検索して取得する  
5 (ステップ172)。なお、認証サーバ5は、予め機器IDとパスフレーズを対応させて記憶している。

次に、認証サーバ5は、サービスサーバ4から受信した認証情報に含まれるサーバ乱数とクライアント乱数を取得する(ステップ174)。

次に、認証サーバ5は、ステップ172で検索したパスフレーズと、  
10 ステップ174で取得したサーバ乱数及びクライアント乱数を組み合わせ、CE機器3と同じロジックにてこれをハッシュ化し、ダイジェストを生成する(ステップ176)。

次に、認証サーバ5は、ステップ176で生成したダイジェストと、  
15 サービスサーバ4から受信した認証情報に含まれるダイジェストを比較し、同一であるか否かを判断する(ステップ178)。

ダイジェストが一致する場合(ステップ180;Y)、認証サーバ5は、CE機器3が認証されたものと判断し(ステップ182)、ダイジェストが一致しない場合(ステップ180;N)、認証サーバ5は、CE機器3が認証されなかったものと判断する(ステップ184)。

20 図8のフローチャートで示した手順では、図4のフローチャートで示したようなワンタイムID1、ワンタイムID2を用いることなく機器認証を行うことができる。

以上に説明した本実施の形態では、以下のような効果を得ることができる。

25 (1) 機器認証モジュール7は、サービスサーバ4が生成したサーバ乱数を用いてパスフレーズをダイジェストに変換した後これを出力するた

め、第三者が機器認証モジュール7の出力からパスフレーズを読み取ることはできない。

(2) 暗号化モジュール8は、機器認証モジュール7からダイジェスト化されたパスフレーズを受信するため、機器認証モジュール7と暗号化モジュール8をスタティックリンクにより結合する必要がない。そのため、機器認証モジュール7と暗号化モジュール8をダイナミックリンクで接続するように構成し、暗号化モジュール8を他のモジュールからも利用できるようにすることができる。

(3) 暗号化モジュール8は、機器認証モジュール7も含め他のモジュールと共に用できるため、暗号化モジュール8を複数用意する必要が無く、CE機器3のシステムの冗長性を解消することができる。そのため、CE機器3のメモリ領域を有効利用することができる。

(4) 認証サーバ5とCE機器3で同じロジックにてダイジェストを生成することにより、CE機器3が生成したダイジェストと認証サーバ5が生成したダイジェストの一致を判断することにより機器認証を行うことができる。

(5) パスフレーズそのものではなく、機器認証ごとに値が変化するダイジェストが通信経路で送受信されるため、例えダイジェストがネットワーク上で第三者に奪取されたとしても、被害を小さい範囲にとどめることができる。即ち、パスフレーズは、機器認証で同じものが何回でも使用できるのに対し、ダイジェストは機器認証ごとに異なるからである。

#### (実施の形態の変形例)

図10は、本実施の形態の変形例を説明するための図である。

図に示したように、本変形例では、機器認証モジュール7を耐タンパチップ35に格納する。

耐タンパチップ35は、集積回路を収納したICチップによって構成

された耐タンパ装置であって、改竄や複製、内部の論理構造の解読などの不正行為に対して十分な防御手段を講じてある。

タンパ (t a m p e r) とは、装置を勝手にいじったり手を加えたりするという意味であり、情報などを不正に変更するという意味もある。

5 耐タンパチップ 35 は、機器 ID とパスフレーズ、及び、パスフレーズとサーバ乱数を組み合わせた情報をハッシュ化するハッシュ化機が内蔵された一種のブラックボックスとなっている。

耐タンパチップ 35 は、耐タンパ仕様で製造されているため、第三者は、耐タンパチップ 35 を物理的に分解して内部の情報を得ることは困  
10 難である。

即ち、耐タンパチップ 35 を物理的に分解して、秘密情報であるパスフレーズや、ハッシュ化に用いるハッシュ関数を知ることは困難である。

また、耐タンパチップ 35 内のパスフレーズは、サーバ乱数と共にハッシュ化されたダイジェストとして出力されるため、耐タンパチップ 3  
15 5 から出力された情報からパスフレーズを解析することも困難である。

即ち、ハッシュ関数は一方向性関数であり、逆変換が困難だからである。

このように、耐タンパチップ 35 の出力情報から内部の秘密情報を探知することも困難である。

図 11 は、本変形例のハードウェア的な構成の一例を示した図である。

20 図に示したように、耐タンパチップ 35 は、バス 24 に接続しており、C P U 21 から情報の入出力を行えるようになっている。

即ち、C P U 21 は、耐タンパチップ 35 に対して、サーバ乱数を入力し、耐タンパチップ 35 から機器 ID とダイジェストを受け取ることができる。

25 以上のように、耐タンパチップ 35 に、パスフレーズ（秘密情報）とハッシュ化機を内蔵し、パスフレーズを出力する際には、ハッシュ化し

たダイジェストを出力することにより、第三者の手にパスフレーズが渡ることを防ぐことができる。

5 このように、耐タンパ装置に、秘密情報とこの秘密情報の変換機能を内蔵し、耐タンパ装置から秘密情報が出力される場合は、変換機能で変換された値が出力されるように構成することにより、秘密情報を物理的、及び解析的に探索することが困難になる。そのため、セキュリティレベルを強化することができる。

10 本変形例では、一例として、耐タンパチップ 35 にパスフレーズとハッシュ化機を内蔵した例について説明したが、この他に、例えば、秘密鍵や共通鍵などの暗号鍵情報を用いるシステムでは、これらの暗号鍵情報と、入力情報に対する署名機能や暗号化機能を耐タンパ装置に内蔵することにより、暗号鍵情報の漏洩を防ぐことができる。

#### 産業上の利用可能性

15 本発明によれば、端末機器内のメモリを有効利用することができる。

## 請求の範囲

1. 機器認証用の秘密情報を備えた端末機器と、前記秘密情報とを用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、

5 前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方向性関数により変換して変換値を生成し、

前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、

10 前記取得した乱数と秘密情報との組を前記端末機器が用いた一方向性関数と同じ一方向性関数により変換して変換値を生成し、

前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システム。

2. 請求項1の機器認証システムで機器認証を受ける端末機器であつ  
15 て、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、

前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

20 前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備したことを特徴とする端末機器。

3. 請求項2に記載の端末機器を機器認証する認証サーバであって、  
25 乱数を取得する乱数取得手段と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に

送信する送信手段と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受け信する受信手段と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

4. 請求項 1 の機器認証システムは、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、

前記サービスサーバは、

乱数を取得する乱数取得手段と、

前記取得した乱数を端末機器に送信する乱数送信手段と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、

前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、

前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、

を具備したことを特徴とするサービスサーバ。

5. 請求項 4 に記載のサービスサーバからサービスの提供を受ける端

末機器であって、

サービスサーバから乱数を受信する乱数受信手段と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

5 前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、  
を具備したことを特徴とする端末機器。

6. 請求項 4 に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバであって、

10 サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

15 前記受信した乱数前記と特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

20 7. 請求項 1 の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、

25 前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、

から構成されたことを特徴とする端末機器方法。

5 8. 請求項2に記載の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、

を備えたコンピュータから構成されており、

10 前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

15 前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、

20 前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、

前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

25 9. 請求項4に記載のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手

段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから構成されており、

前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信  
5ステップと、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定  
ステップと、

10 前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、

前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、

15 から構成されたことを特徴とする認証方法。

10. 請求項4に記載のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、

20 前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、

前記受信した乱数と、秘密情報の組を前記変換手段で一方向性関数により変換して変換値を生成する変換ステップと、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定する  
25 ための秘密情報特定情報を前記送信手段で送信する送信ステップと、  
から構成されたことを特徴とする端末機器方法。

11. 請求項4に記載のサービスサーバがサービスを提供する際に、  
端末機器を機器認証する認証サーバが用いる認証方法であって、前記認  
証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証  
手段と、を備えたコンピュータから構成されており、

5 サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる  
認証情報を前記受信手段で受信する受信ステップと、

前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前  
記端末機器の秘密情報を特定する秘密情報特定ステップと、

10 前記受信した乱数前記と特定した秘密情報との組を前記変換手段で前  
記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生  
成する変換ステップと、

前記機器認証手段で、前記受信した変換値と前記生成した変換値を用  
いて前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

15 12. 請求項1の機器認証システムで機器認証を受けるコンピュータ  
で構成された端末機器において、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する  
受信機能と、

20 前記受信した乱数と秘密情報の組を一方向性関数により変換して変換  
値を生成する変換機能と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバに  
おいて前記秘密情報を特定するための秘密情報特定情報を送信する送信  
機能と、

を実現する端末機器プログラム。

25 13. 請求項2に記載の端末機器を機器認証するコンピュータで構成  
された認証サーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信機能と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報5受信する受信機能と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

10 前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

を実現する認証プログラム。

15 14. 請求項4に記載のコンピュータで構成されたサービスサーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数を端末機器に送信する乱数送信機能と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報20受信する受信機能と、

前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信機能と、

前記認証サーバから前記送信した認証情報による認証結果を受信する25認証結果受信機能と、

を実現するサービスサーバプログラム。

15. 請求項4に記載のサービスサーバからサービスの提供を受けるコンピュータで構成された端末機器において、

サービスサーバから乱数を受信する乱数受信機能と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、

を実現する端末機器プログラム。

16. 請求項4に記載のサービスサーバがサービスを提供する際に、

10 端末機器を機器認証するコンピュータで構成された認証サーバにおいて、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

15 前記受信した乱数前記と特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

20 を実現する認証プログラム。

17. 請求項12、又は請求項15に記載の端末機器プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

18. 請求項13、又は請求項16に記載の認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

25 19. 請求項14に記載のサービスサーバプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

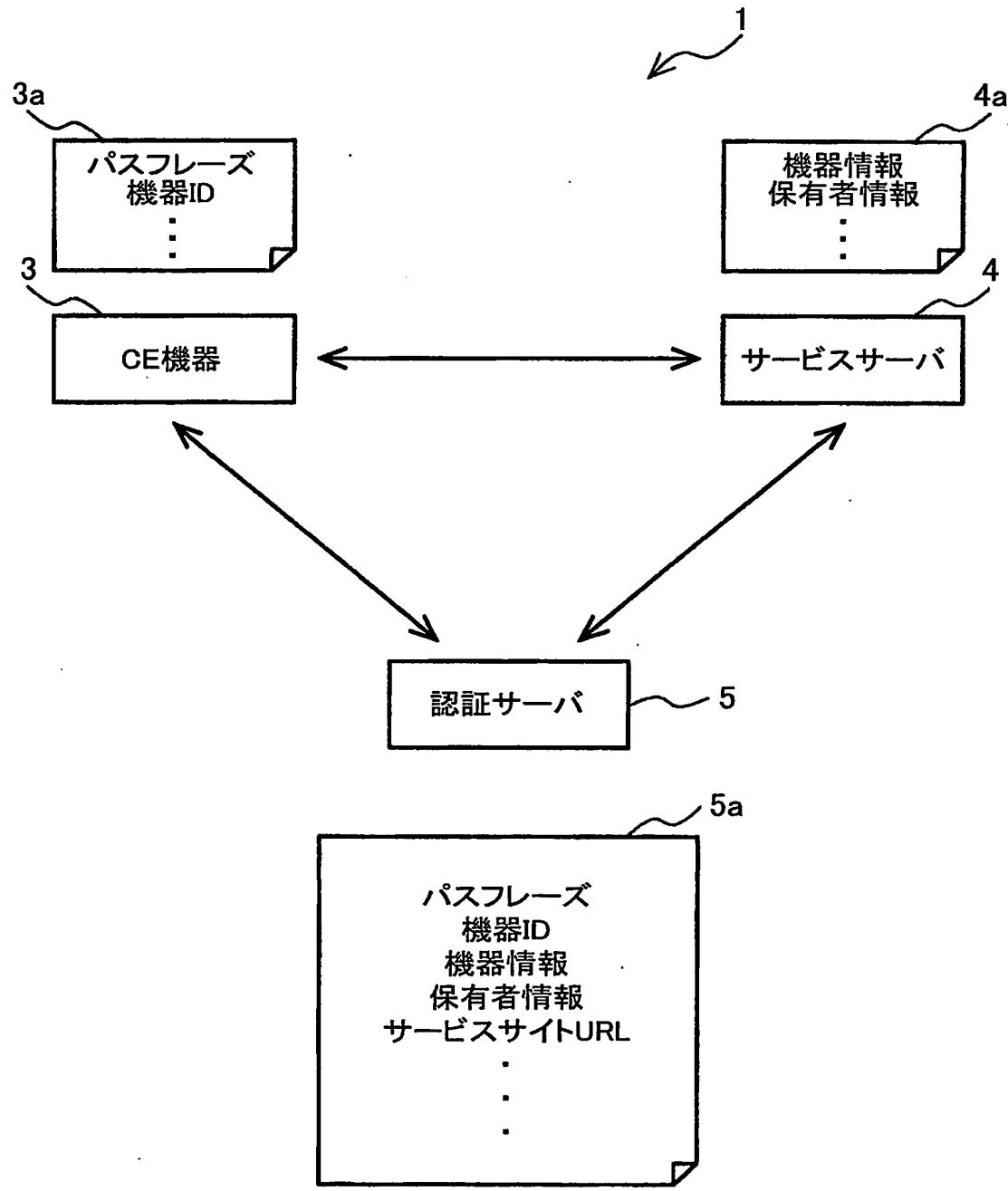


Fig.1

2/9

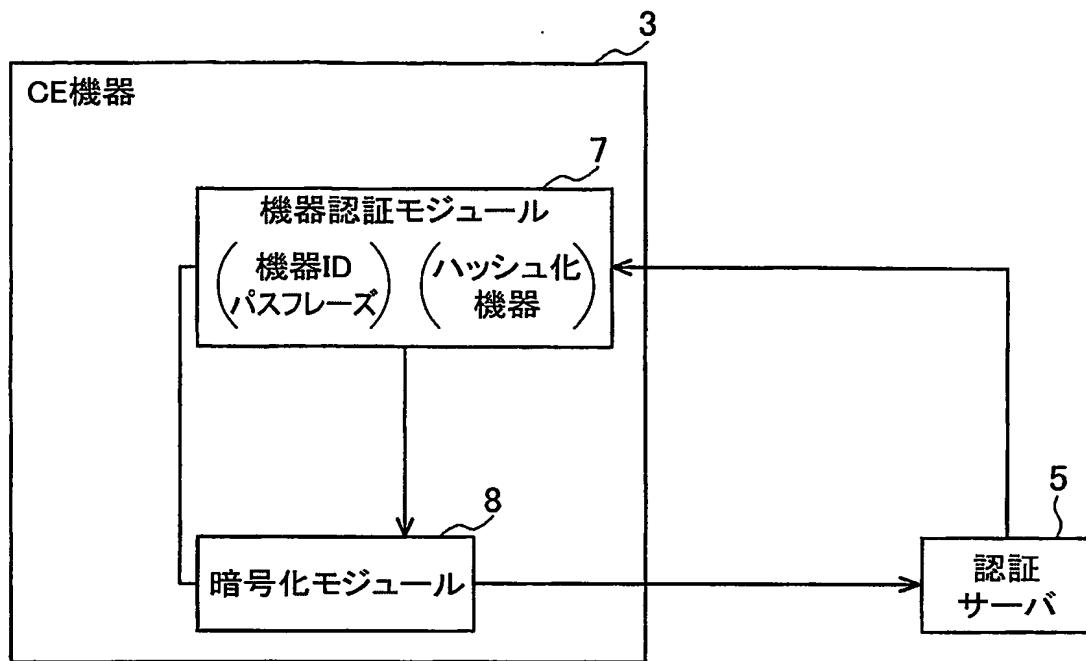


Fig.2

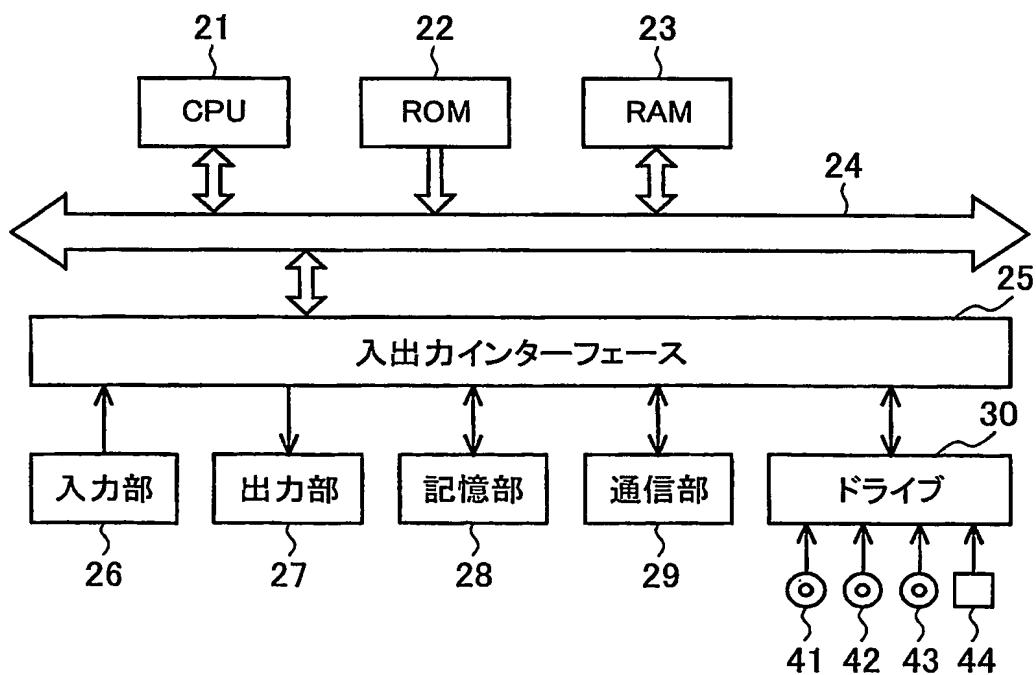


Fig.3

3/9

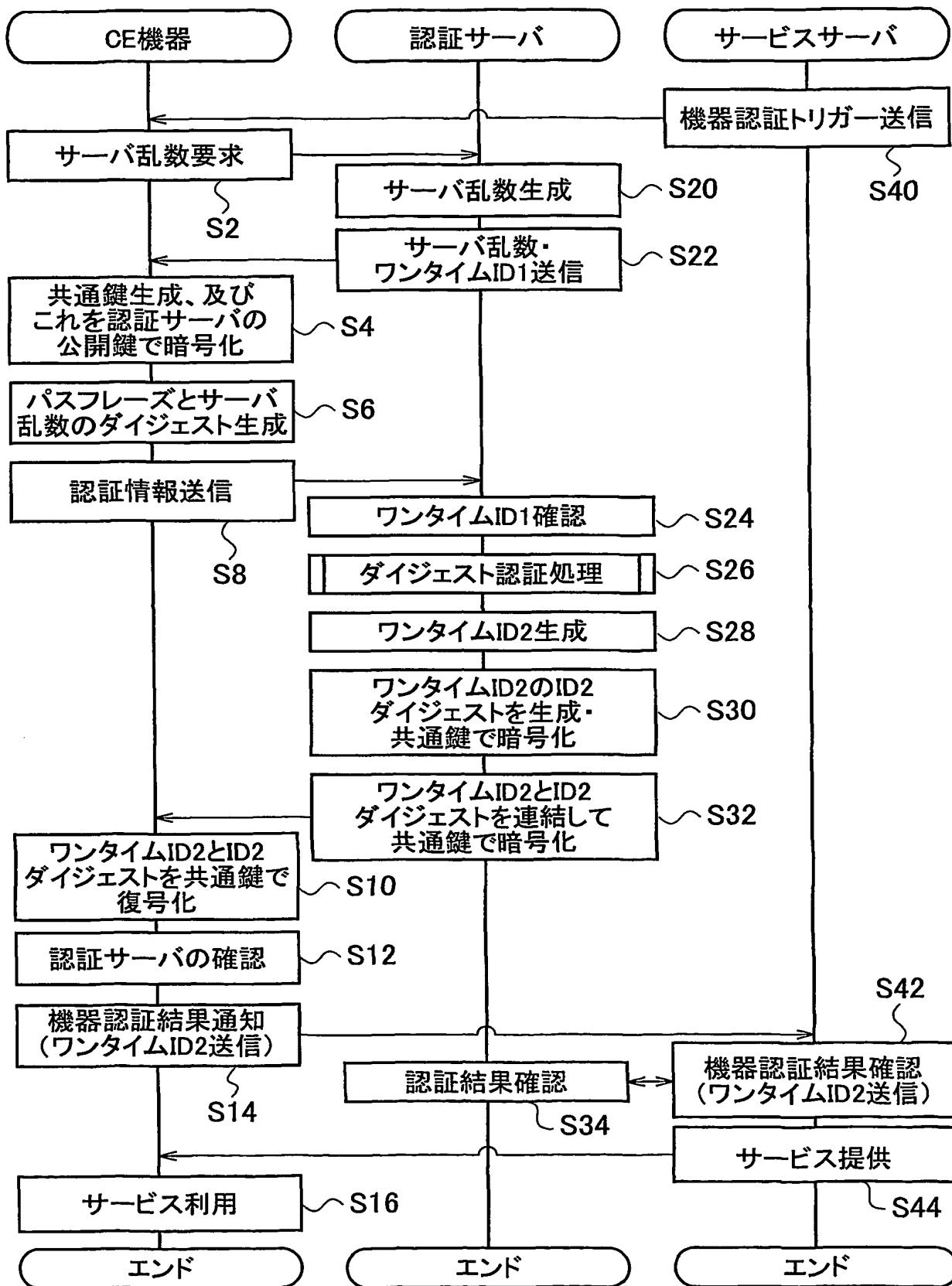


Fig.4

4/9

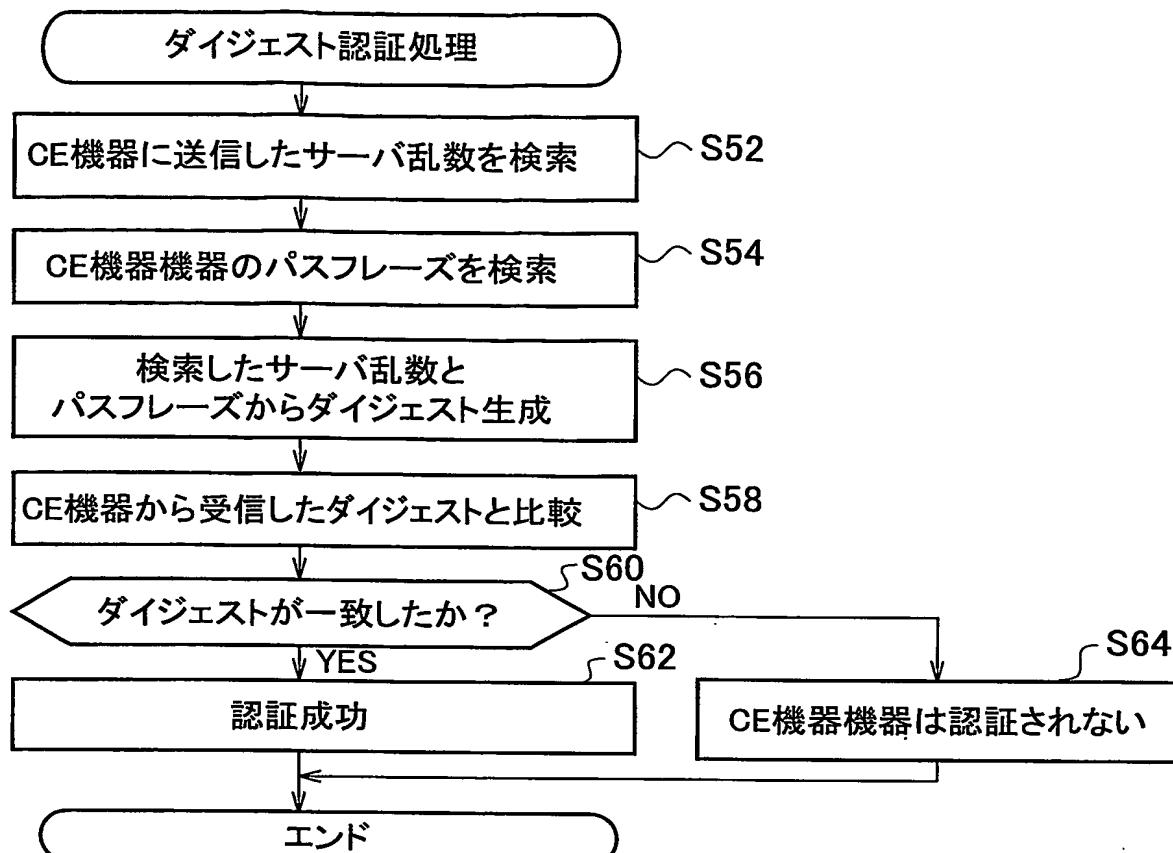


Fig.5

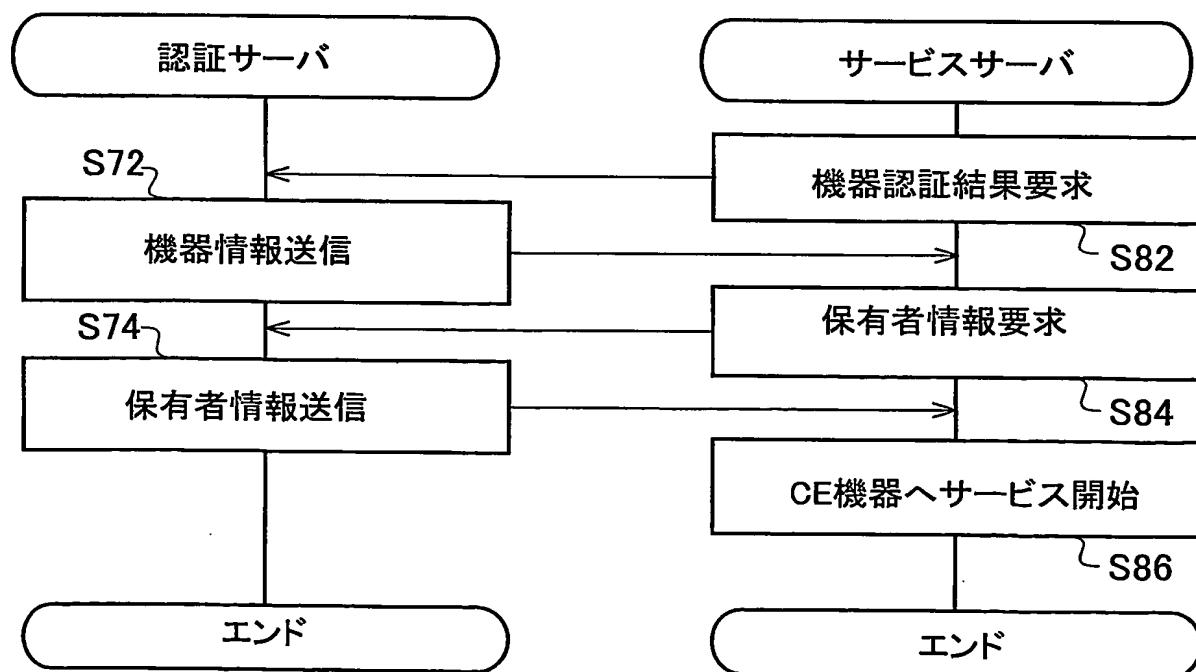


Fig.6

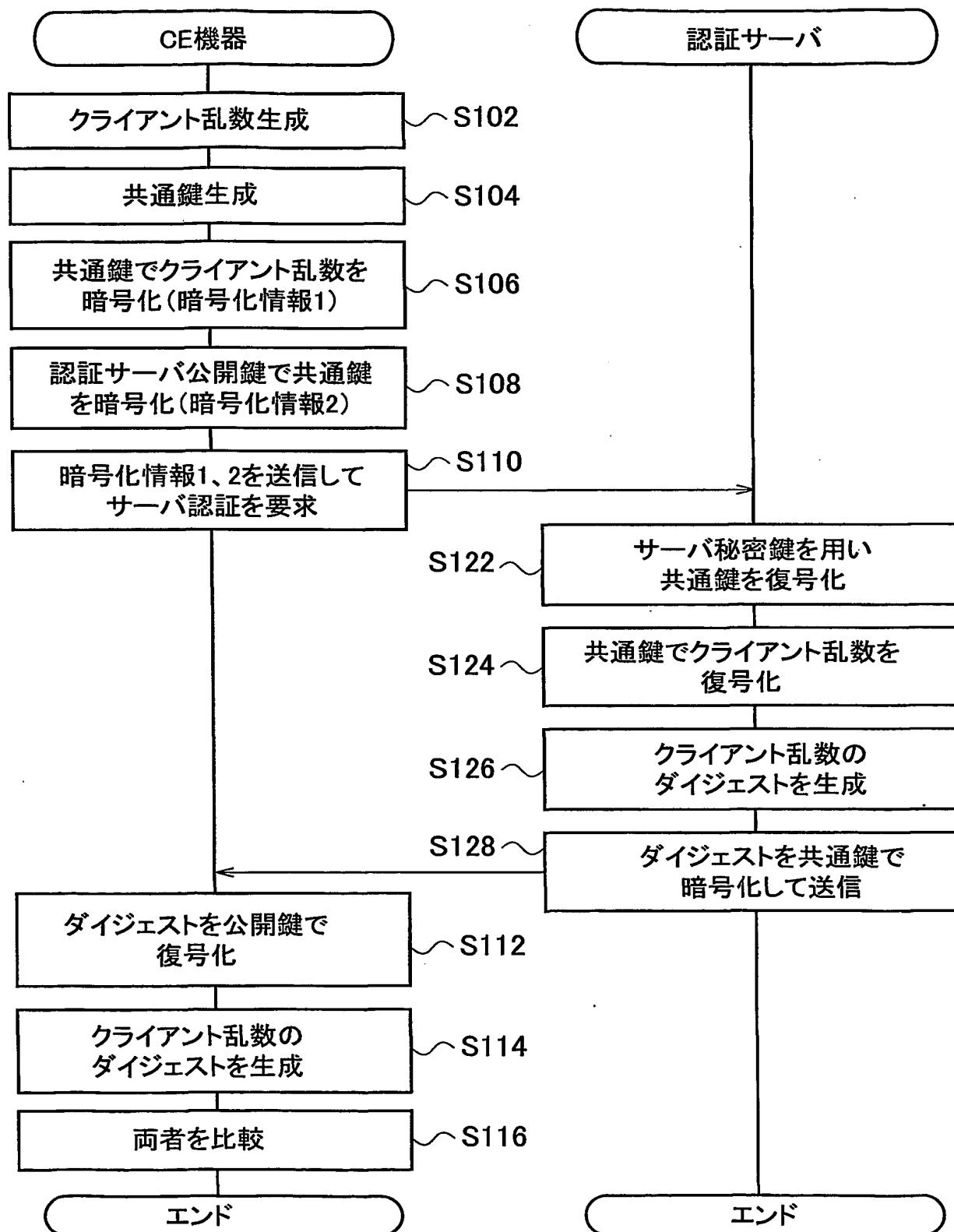


Fig.7

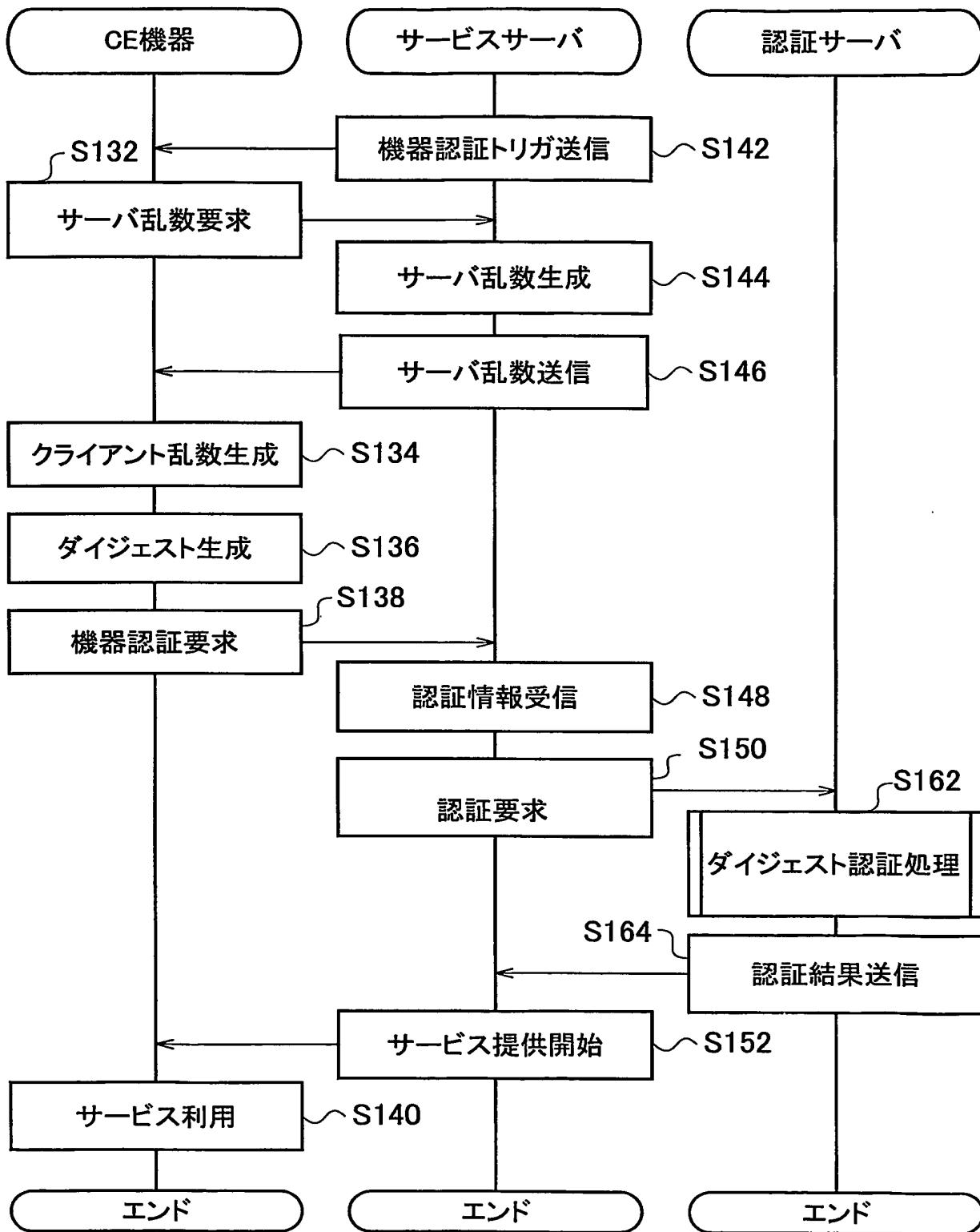


Fig.8

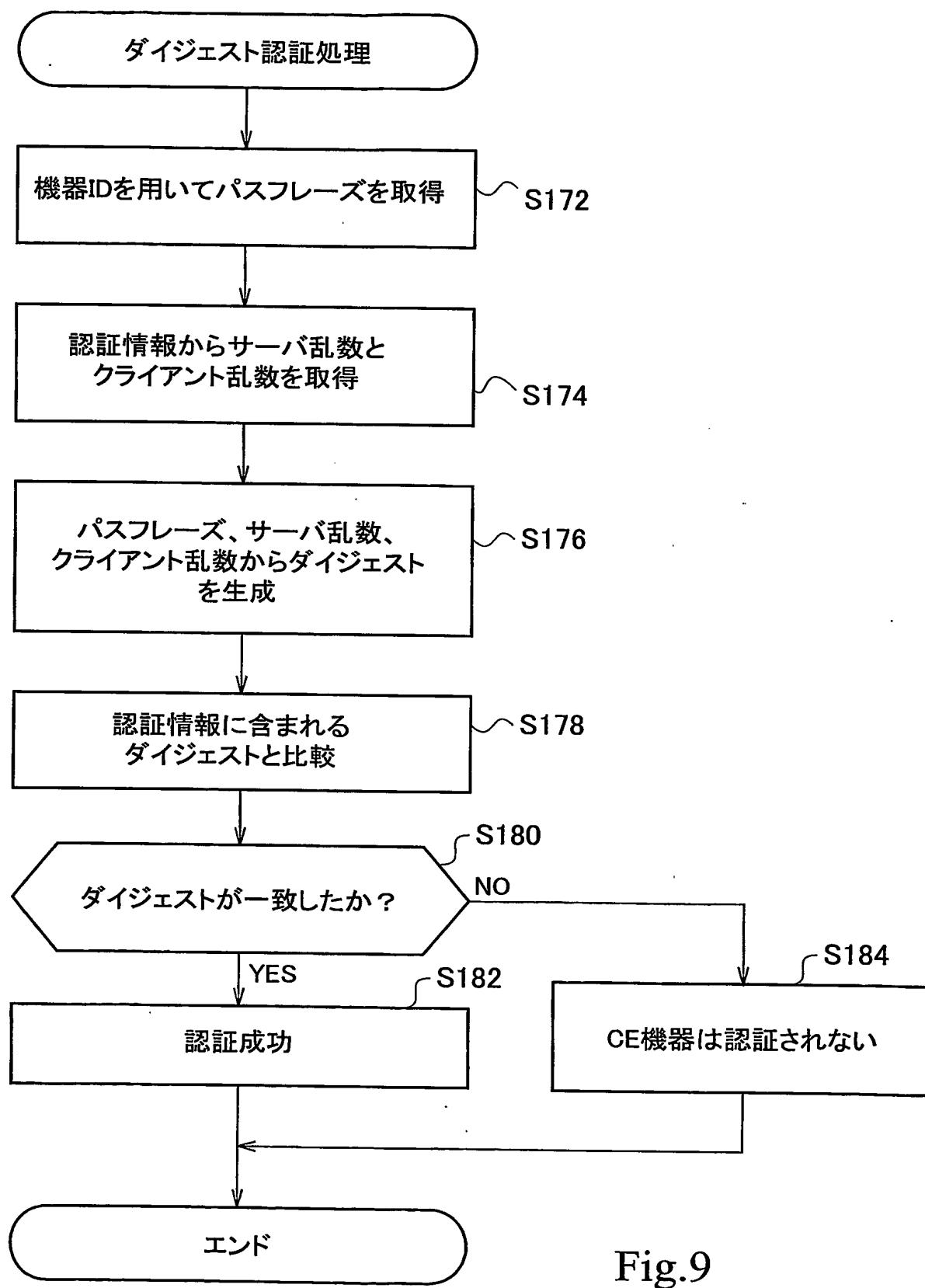


Fig.9

8/9

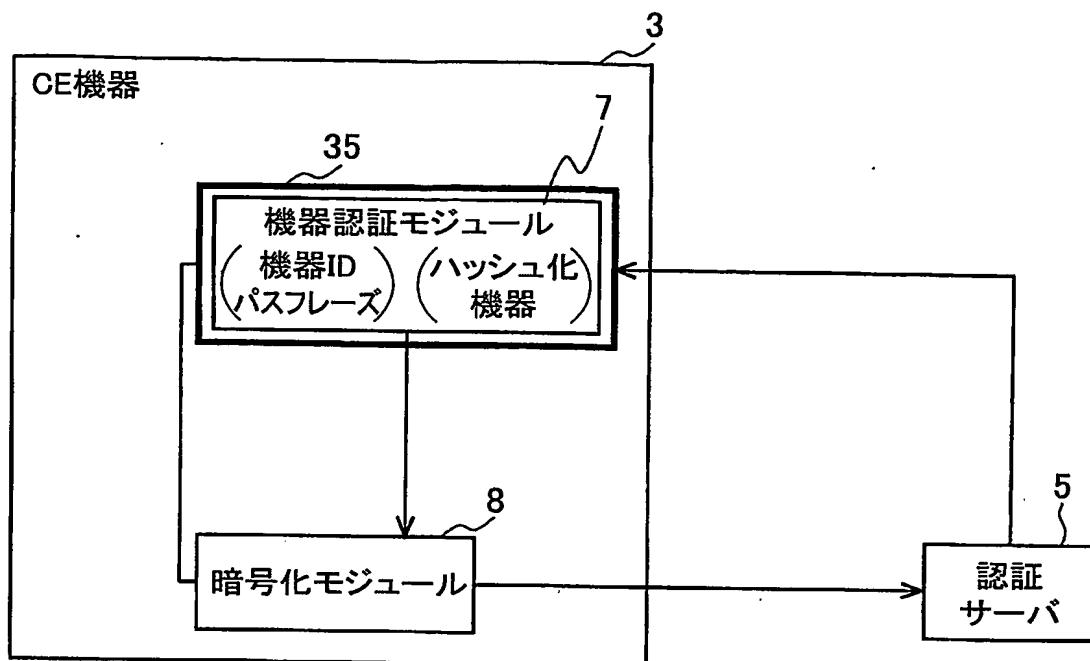


Fig.10

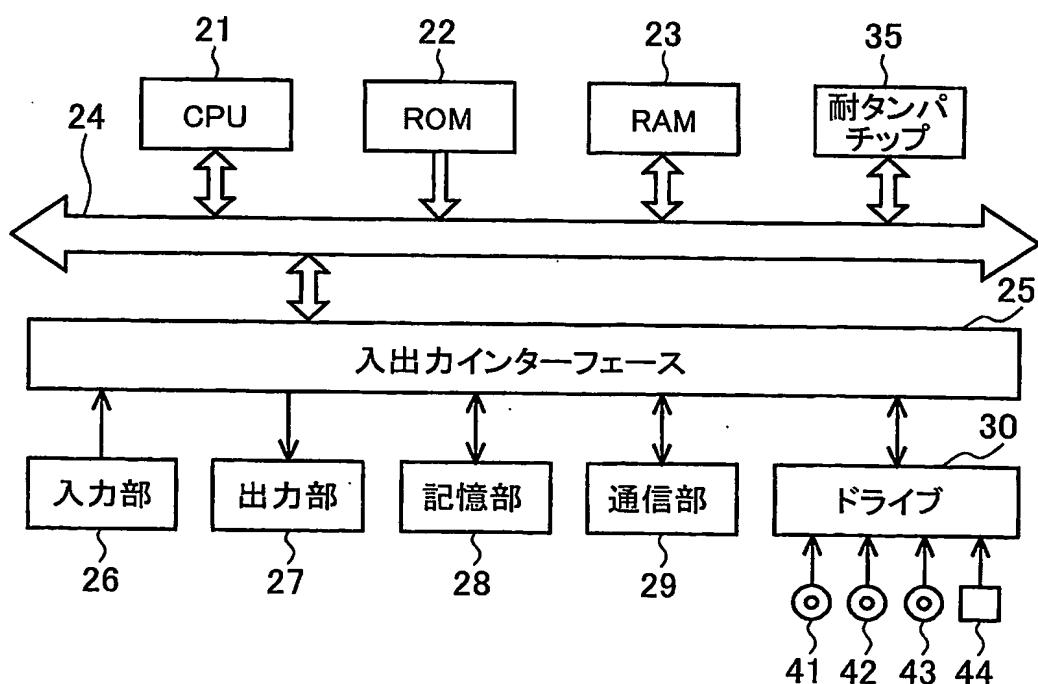


Fig.11

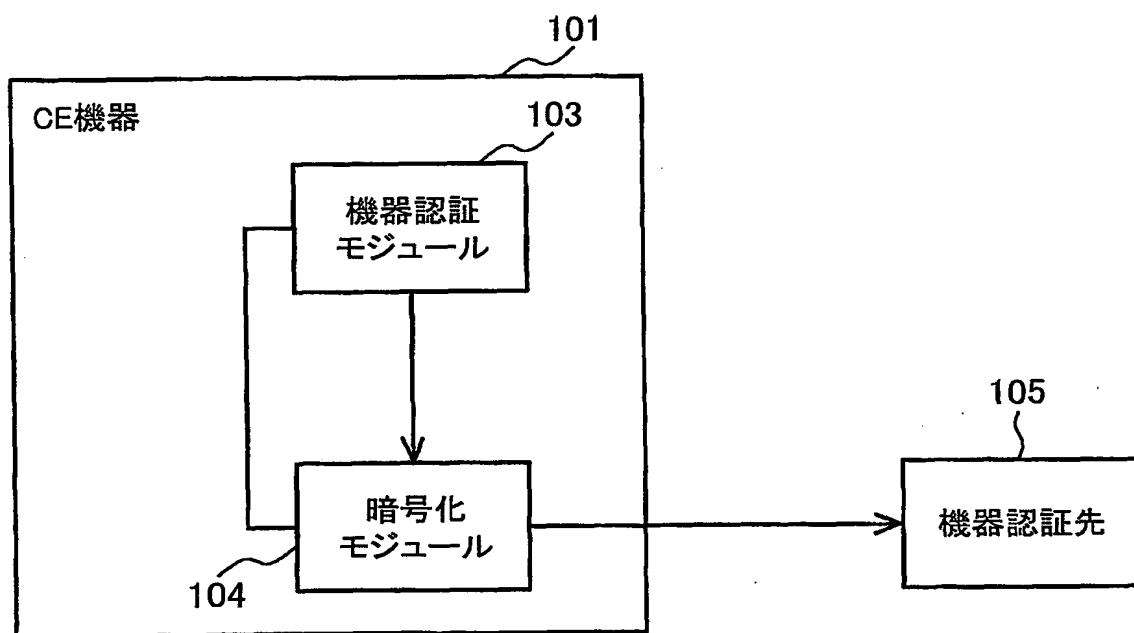


Fig.12

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005741

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/32, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/32, G06F15/00Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 11-316729 A (Nippon Telegraph And Telephone Corp.), 16 November, 1999 (16.11.99), Par. Nos. [0032] to [0038]; Fig. 5 & EP 921487 A & US 6343284 B	1

 Further documents are listed in the continuation of Box C. See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
21 May, 2004 (21.05.04)Date of mailing of the international search report  
08 June, 2004 (08.06.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2004/005741

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.: 2-19  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:  
  
(See extra sheet.)
  
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

The additional search fees were accompanied by the applicant's protest.  
 No protest accompanied the payment of additional search fees.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/005741

Continuation of Box No.II-2 of continuation of first sheet(2)

The scope of claim 2 contains a description of "a terminal device receiving a device authentication by the device authentication system of claim 1 characterized in that ..... Herein, even if "claim 1" means "the scope of claim 1", "the scope of dependent claim" is "the scope of claim" containing all the features of one or more other scopes of claims (PCT Rule 6.4 (a)). However, "a terminal device" cannot have all the features of the "device authentication system". Accordingly, the scope of claim 2 cannot be the scope of claim dependent on claim 1. Moreover, it is unclear what kind of meaning is contained in the technical feature that the terminal device receives a device authentication from a device authentication system characterized by performing authentication by a particular procedure when specifying the "terminal device". Accordingly, such a description makes unclear the feature for specifying the invention.

The same applies to the scopes of claims 3-19.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. C I' H 0 4 L 9 / 3 2, G 0 6 F 1 5 / 0 0

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. C I' H 0 4 L 9 / 3 2, G 0 6 F 1 5 / 0 0

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 11-316729 A (日本電信電話株式会社) 1999.11.16, 段落【0032】-【0038】、図5 & EP 921487 A & US 6343284 B	1

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」口頭による開示、使用、展示等に言及する文献  
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」同一パテントファミリー文献

## 国際調査を完了した日

21. 05. 2004

## 国際調査報告の発送日

08. 6. 2004

## 国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

## 特許庁審査官 (権限のある職員)

中里 裕正

5M 3365

電話番号 03-3581-1101 内線 3597

## 第1ページの続葉（2）第II欄 2. のつづき

請求の範囲第2項には、「請求項1の機器認証システムで機器認証を受ける端末装置であつて、...端末装置」と記載されている。ここで、「請求項1」なるものが、「請求の範囲第1項」の意味であるにしても、「従属請求の範囲」とは、1又は2以上の他の請求の範囲の全ての特徴を含む請求の範囲である（PCT規則6.4(a)）ところ、「端末装置」が

「機器認証システム」の全ての特徴を含むはずも無いから、かかる請求の範囲第2項は、請求の範囲第1項の従属請求の範囲ではない。そして、端末装置が、特定の手続きにて認証を行うことを特徴とする機器認証システムで機器認証を受けるものであるということが、「端末装置」を特定する上でどのような意味を有するのか不明であるから、かかる記載は発明を特定するための事項を著しく不明確にするものである。

請求の範囲第3-19項についても同様である。

## 第II欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1.  請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。  
つまり、
2.  請求の範囲 2-19 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、  
別紙参照。
3.  請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第III欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1.  出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2.  追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3.  出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4.  出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- 追加調査手数料の納付と共に出願人から異議申立てがあった。
- 追加調査手数料の納付と共に出願人から異議申立てがなかった。